Some considerations on cyberspace law

Poullet, Yves

Published in:
The international dimensions of cyberspace law

Publication date:
2000

Document Version
Publisher's PDF, also known as Version of record

1 Some Considerations on Cyberspace Law[1]

YVES POULLET

> ... We should like to stress the State's vital obligation to intervene at a time when, in our opinion, deserting the Internet and withdrawing from the field of regulation to such a point that it no longer even decides the general framework, would notably put at risk public order, fundamental liberties and other basic values.[2]

INTRODUCTION

The Characteristics of Cyberspace

'As cyberspace develops increasingly into a zone of human exchange, the need for balanced and well-adapted rules of the game gains in importance.'[3] Are these rules new? Opinion has long held that the Internet revolution has to be matched by a revolution in law. As noted by the Working Document of the Expert Meeting on Cyberspace Law which took place in Monte Carlo in September 1998:

> In this respect, the most authoritative legal writers admit that today's Internet revolution, which will be confirmed by tomorrow's information society, must in any case be matched by a revolution in the law in the broad sense of the term.[4]

Two characteristics of cyberspace have been amply highlighted in this context. First, cyberspace ignores frontiers: yet law, which is based essentially on the notion of territorial states, is intended for the control of situations that are localized. 'Cyberspace calls into question frontiers, which it bypasses, and the state laws, which it challenges.'[5]

Second, cyberspace is never confined, but is continually being redefined to favour the hyperlinks of its users. The distinctions with

which law seeks to regulate communication begin to melt when faced with such infinite possibilities:[6] distinctions separating the parties themselves, at a time when anyone may be producer, intermediary and consumer of information simultaneously; distinctions of media, at a time when written text, printed text and sound are becoming mixed; and classical opposition between the products' regulations and the services' regulations at a time when digitalization of the so-called 'informational products' make this distinction inoperative and dangerous. Moreover, the concept of a 'work' need no longer be linked to a person and a particular medium but simply to an object and a process in which any number of persons may be involved. Finally, the distinctions between communication in the public and private domains are becoming increasingly blurred.

Thus the 'natural' place for the intervention of law and the structures and concepts that govern its operation are vanishing into our 'global village'.[7]

The Aims of this Chapter

This chapter is intended to explore a number of ideas on the basis of the position outlined above.

The first section is intended to make jurists aware that the latest developments in technology and communications not only call for an expansion of traditional concepts but, beyond this, frequently modify the system of checks and balances enshrined at their heart, thereby giving rise to new demands for legislation.

Following on from this, questions are raised on the means by which law is created in a modern context. There is a great temptation to hand over the task of legislating social behaviour in cyberspace to self-regulation and regulatory technology. This gives rise to questions on the role of the state and the potential dialogue between different norms, state regulations and self-regulations.

Finally, the values with which the law should be concerned with promoting so that our society may be both informational and democratic are discussed.

A LAW ON THE BRINK: FROM GROWING CONCEPT TO WIDENING DEBATE

Digitalized, flashed across vast distances via world-embracing networks, processed in a variety of ways and transferred from one medium to another, information is becoming uncontrollable. From the legal viewpoint it is breaking the confines of tradition in every

way. The restraining duty of the jurist – in other words, his or her obligation to confront novelty with ancient concepts and their associated values, is in natural opposition to such an explosion; he or she abides by an established concept until analysis reveals, clearly and evidently, either the impossibility of its satisfaction or the necessity, induced by a new disequilibrium, of protecting new values.[8]

Two debates illustrate this: the first concerns the electronic signature, while the second considers the consequences of so-called Electronic Copyright Management Systems (ECMS). The conclusions drawn from these two examples will serve to highlight certain reflections on the meeting of law and technology.

Signatures in all their Forms

Expanding the Law: A Functional Approach

The problem of an electronic signature's validity seems, since the works of UNCITRAL[9] and European Draft Directive 98/297/EC on a common framework for electronic signatures, to have been resolved by way of a functional approach. The answer to the question 'Should we profoundly alter our legislation to admit the reality of computers and communications technology?' was in the negative. The 'providential' openness of the legal concept of the signature permits the inclusion of this new reality by demanding the technical means for the creation and appending of an electronic signature, the same practical demands as are placed upon its handwritten equivalent – the signatory's identification and the authentification of a document to which his or her signature must remain attached. Thus, as we are frequently made aware, the development of information technologies is an opportunity for the revitalization of traditional concepts. The danger of ad hoc solutions must be emphasized: despite the advantage of apparent simplicity, they can create long-term turbulence in jurisprudence.

Previous attempts to legitimize electronic proof by means of exceptions to the signed document principle have proved ill-fated. Such solutions showed their limitations whenever particular laws called for a hand-signed document and, more seriously, encouraged an over generous acceptance of electronic proof, without demanding sufficient security requirements in its creation. That said, the idea of an equivalence in principle between manuscript and electronic signatures certainly does not close the debate. Many other questions may be asked beyond the narrow regulatory bracket in which, until now, the legal dispositions covering the legal issue of the signature alone have been inscribed. The points developed below illustrate the necessity of extending this debate.

Technical Normalization: Society's Risks

The first question takes us back to the statute and the setting up of norms. The actual requirements to be met by an electronic signature before it can pretend to the quality of its handwritten counterpart develop as technological evolution advances. Thus the robustness of a signature, if it is to serve as proof of identification, presupposes the use of ever more perfect and secure methods of cryptography.

> The content of such requirements must develop in accordance with technological evolution and the functions drawn from each concept. There can be no question of defining, once and for all, on the basis of a given state of technological development, the precise implications of each of these functions. Thus the robustness of a signature may suppose the use of ever more perfect and secure methods of cryptography.[10]

The difficulty that a company or administrative authority, wishing to take advantage of electronic proof, faces in demonstrating the quality of its security measures can readily be imagined. This leads inevitably to movements towards standardization in the context of ad hoc public or, more frequently, private institutions. This normalization, without being obligatory, nonetheless represents a standard acceptable to the courts, with the reservation of such expert evaluation as these may consider appropriate. The advantage of such normalization is its relative flexibility. Openness to the possibility of participation in such a normalization process, also by consumer representatives, would be advantageous (compare, on this matter, the statutes of the ETSI).

Questions of system interoperability and the laws of competitive trading are closely linked to the issue of technical norms. The normalization of a particular cryptographic system may enable a company to corner a market. We must bear in mind the requirements of 'transparency' in normalization and the need for legislation permitting every operator to enjoy this 'essential facility'.

Finally, the development of the cryptographic procedures that underlie electronic signatures gives rise to other concerns: legitimate public security issues permit wire- and phone-tapping under certain strict procedural conditions. What will happen to this legitimate state security concern if undecipherable messages are circulating on the information superhighways of tomorrow? This sensitive discussion provided the backdrop to the OECD guidelines on cryptography which were adopted on 27 March 1997.

The Question of Fundamental Rights

The growing demand for a move to electronic signatures for access to all kinds of services, including government online services, raises other questions – namely, the right of every citizen to an electronic signature and to sign anonymously, the corollary right to request that government authorities maintain paper procedures for 'cyber have-nots' and, finally, the right to use several signatures in order to avoid the signature becoming a unique identification liable to be subjected to numerous processes.[11] The Meeting of Experts on Cyberspace Law convened by the UNESCO Director-General in 1998 underlines, in Principle No. 8, the importance of the fundamental right of every person to privacy, including the right to communicate confidentially using certain techniques such as cryptographic systems and pseudonyms.

A New Role for the Signature

There are two aspects to this: first, recognition that the electronic signature will cause the emergence of new agents whose services may require regulation and, second, the fact that the electronic signature functions in a different manner to its manuscript cousin.

Regarding the first point, electronic signature technology, which is based on asymmetric cryptography, requires the intervention of new parties, particularly certification authorities responsible for publishing signatories' public codes in open registers and guaranteeing their authenticity of content. Their work will be the object of new regulations establishing their responsibilities and fixing the conditions for the official recognition of their activities.

As to the second point, the disappearance of exchanges based on the physical proximity of parties whose identities are previously known to one another, in favour of transactions concluded across non-territorial virtual space, fundamentally changes the very nature of contractual relations. This has repercussions, notably on the function of the signature which can no longer be perceived simply as the *a posteriori* confirmation of a transaction for the purposes of proof. The signature itself becomes a condition for the recognition of the contractual parties and therefore a prior condition for the drawing up of a transaction.

Must this recognition necessarily be that of an individual, or can it be that of a legal entity? What the manuscript signature did not permit yesterday can now be authorized by the electronic signature. A legal entity may, in future, dispose of a signature in the fullest sense of the term and be able to initiate operations without recourse to an individual signatory; this will be especially true of automatic systems dealing with ordering and invoicing.

Preliminary Conclusions: The Fracturing of Disciplinary Boundaries

To conclude, electronic signature law certainly invites us to revisit the law in this new light, expanding traditional concepts and, beyond this, exploding the disciplinary divisions of law. The signature, classically a question of civil contract law, veers into the field of human rights with such issues as the right to a signature, the right to eavesdrop electronically, and the protection of privacy, as well as into the field of fair trade law with the right to free competition and the issue of establishing norms. The second example highlights the dual concern confronting the jurist involved in information and communications technology: the need to reread the law and to be aware of the fracturing of disciplinary boundaries that the legal recognition of information and communications technologies provokes.

ECMS or the Death of Copyright?

Electronic Copyright Management Systems (ECMS)

The Internet is clearly no longer the grand university forum of ideas celebrated at the time of its creation, but is becoming daily more and more like a trade fair. Cryptographic systems and signatures and, more generally, such technological methods as 'tattooing' permit control of, and limited access to, information that is better protected by these means than it would be in a bank vault.[12]

Such systems, among which can be found programs for managing 'works', substitute for the protection classically assured by copyright, or more recently by other rights considered *sui generis*. They provide far more effective technical and contractual protection not only to works effectively protected by the Act, but equally well to types of information not previously afforded any legal cover.[13]

Towards the Death of Copyright

It would certainly be useful to ask what the legal limits of protection technology are.[14] Such systems render the protection by judicial regime irrelevant, assuring the holders of simple informational property protection of a degree and effectiveness beyond the measure commonly accorded by rights of intellectual property, with the exception of the sacred principle of the free circulation of ideas.

What is to become of, *inter alia*, the right of quotation, the exceptions for the benefit of scientific research, and copying for personal use and education if technology is capable of blocking all non-contractual use? Would it not be more appropriate, rather than

bemoaning the demise of the laws of intellectual copyright, to insist instead that technology should conform to them?[15] The rights of quotation, the rights of scientific researchers and the right of copying for private use must be specifically recognized, however advanced technical protection may become. More fundamentally, the abovementioned Expert Group brought together by UNESCO at the second Monte Carlo Info-Ethics Conference (September 1998) stressed that:

> Public bodies should have an affirmative responsibility to make public information widely available on the Internet and to ensure the accuracy and timeliness of the information. This information could include government information, information concerning cultural heritage, and archival and historical information .... States should preserve and expand the public domain in cyberspace.[16]

The development of vast ECMS systems invites further reflection. Who runs these systems? What role should be granted to copyright protection agencies? Once again, questions of fair trade and normalization, particularly with respect to the encryption of works, are sure to be raised.

Finally, the use of such systems will generate nominative data, and it will become important to determine what rights to the exploitation of this data will be granted to the various parties, from the system operators to the authors themselves.

From a Service to an Information Product

I will approach the issues relative to this second example via certain remarks on the subject of the responsibilities involved in online data banking.

Traditionally speaking, the supplying of information was regarded as a service, the service provider being obliged to deliver the required dispatch to his client. The introduction, between the producer of information and the internaut, of a technical tool capable of responding in a standard way to varied demands for information pushes us towards another analysis of the process and, as recent jurisprudence demonstrates, to question – in the case of incomplete or inexact information – the very quality of the 'data product'. By 'data product' we understand the entirety, including both the technical (software and programming) and organizational means (collection method and sample quality), as well as content (integrity, contemporary nature). It becomes an issue of the conformity of the product to the internaut's expectations.[17]

Clearly, the online information service producer and distributor must now view their responsibility in terms of product quality and no longer in terms of delivery.

Site Labelling and Filter Techniques

Technology comes to rescue the law. It is in this context that we can explain the tendency to develop labelling techniques (such as Webtrust and Trust-e), just as for conventional consumer products and, building on this, to introduce filter systems such as Platform for Internet Content Selection (PICS) and even negotiating systems like Platform for Privacy Preferences (P3P). The idea is simple. Every 'data product' can be examined for its conformity to threshold standards for decency, violence, respect for privacy (compare, in this regard, Trust-e), consumer protection and so forth. Such labelling would operate *a priori* in connection with filter techniques enabling the internaut to select sites according to personal preference and even to negotiate with these sites an individual protection or, conversely, discard it.[18]

Undoubtedly, labelling laws still have to be drawn up: what criteria would decide which sites required labelling? Can we even envisage contesting criteria? What degree of transparency must be expected of the criteria? What will be the responsibilities of labelling authorities? What legal recognition should be granted to such labels? What role has the state to play as regards the recognition of the labelling authorities? And, finally, what private or public sanctions should be levied for failure to respect the conditions applied?[19]

Second Conclusions: On the Interaction Between Law and Technology

We must admit that technology can strengthen the law's effectiveness and that, without such reinforcement, it would either become a dead letter or be poorly served by classic judicial procedures that are neither rapid nor effective. A revisionist site would certainly be better countered by such mechanisms as filtering or blocking its access, as envisaged by the 'Internet Charter', than it would be by the condemnation by a tribunal of something that is essentially unseizable and currently sailing somewhere far out on the global chart of the World Wide Web. In another order of ideas, as indicated above, ECMS are more effective than legislation at protecting an author's copyright. All these remarks support the opinions of certain authors[20] that the so-called *lex informatica* – that is, regulation by technical means – is preferable to classic legal ones.

When this argument is stretched to highlight the various facets of this legal–technological axis, it is clear that it is as much the parties themselves who are calling for legal measures to legitimize technical solutions as it is the law calling on the parties to take whatever technical measures are necessary to ensure its effective respect.[21]

The former role – that of legitimizing technical solutions – is definitely the one being sought by the promoters of Internet services.

The electronic signature, as the first example analysed, demonstrates the need for security in commercial relationships on an open network such as the Internet; it also justifies service providers' requests for legal recognition of electronic certification services – those famous electronic notaries known as the 'certification authorities' or 'trusted third parties' such as Belsign or Isabel whose activities have already been legalized in some states (Germany, Italy and the United States) and will shortly be so in others. As regards ECMS, the recent reform of the Berne Convention on authors' rights criminalizes any attempt to outwit the technological protection systems offered by copyright management services.

On the other hand, the law may call for either direct or indirect technical measures to be taken. Applying the principle of responsibility could lead a judge to sanction, in either a civil or a criminal suit, access providers and servers who have not taken currently acceptable and appropriate technical measures to prevent possible harm to clients using their services. It is in response to such fears, and particularly the fear of a legislative intervention: in the form of a 'Decency Act' that American industrialists and others have developed the filter standard known as the Platform for Internet Content Selection (PICS) (see above).

It is important that lawyers should carefully examine the 'privacy', 'copyright', and 'consumer protection' enhancing technologies to ensure that they strictly conform to both the letter and the spirit of the law. This is not always the case: thus ECMS do not always operate in accordance with the equilibrium established by copyright legislation between the interested parties. Similarly, in the case of 'privacy enhancing technology', the P3P system would permit the user to negotiate his or her right to privacy, including rights that are not negotiable, being directly linked to fundamental liberties.[22] In other words, the technology should comply with the law.

THE VARIOUS REGULATORY TECHNIQUES ON THE INTERNET AND THE ROLE OF STATE LAW

Clearly, technology can serve to regulate behaviour on the information superhighway. However, there are other regulatory models with which the law may even maintain a dialogue.

Below, I first identify the different regulatory techniques applicable to the Internet or to information superhighways in general; I then analyse the various responses in state and supranational law to these different regulatory techniques and envisage some criteria for the legitimization of non-state regulatory systems.

On the Diversity of Regulatory Models

Preliminary Considerations

The goal of regulation is the prescription of behavioural norms. That said, the diversity of regulatory models and the application of norms could be divided into four categories: the object, the author, the subject and the sanction of the norm.

We may note at the outset that the international dimension of the Internet leads to a degree of competition between different national regulations. As soon as one country decides to regulate certain activities, the parties concerned by the legislation are free to move their activities to another country with a more flexible and less strict regulatory framework. This phenomenon of 'regulatory dumping' is real.[23] On the other hand, advantages can accrue to the consumer who prefers the security that is granted by a regulatory environment that takes better care of his or her interests. This second aspect should not be neglected.

An Enumeration

It is impossible to number all the many normative sources of law on the Internet. Those public sources of law – the national state and international norms – contrast with the private ones, based either on contractual liberty or on the sort that tends to be called self-regulatory; one may now distinguish aspects of certification and usage that some regard as an emerging *lex electronica*, parallel to *lex mercatoria* but developed within an electronic context. The technology itself (see 'Second conclusions', p.154 above) may also have a normative effect on behaviour.

As regards these private sources, we may observe that the actors themselves have developed means to ensure that the self-regulatory code passes from the letter into action. Thus the coordinators nominated within discussion groups are expected to vet incoming messages. The sanctions peculiar to the network, such as disconnection and 'flaming', are strangely reminiscent of vigilante justice. The hotlines created within the framework of certain codes of conduct to permit the denunciation of activities contrary to those codes are a further example of the means put in place to assure adherence to network discipline. More interesting still are the labelling and rating mechanisms developed by certain servers (see 'Site labelling and filtering techniques' p.154 above) which both guarantee and inform the user of the quality of the service being offered (such as the 'privacy-friendly' label or the one relating to web sites of journalistic information on respect for the press code). Naturally, the value of any such classification depends on the certifying body which defines, issues and controls it. It is appropriate to mention the North American initiative to create 'virtual magistrates', online arbitrators or mediators who are authorized to adjudicate conflicts arising out of network use, whether they concern matters of defamation, intrusion into the private sphere or non-respect of the rules of a news group. These alternative dispute resolution (ADR) mechanisms have recently been promoted by the European Draft Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market.

Briefly, we can see that private regulatory sources set up their own mechanisms for expressing the rules, controlling their application and, finally, sanctioning non-respect; such sanctions are pronounced by their own 'magistrates'. The following reflections will develop certain summarizing remarks concerning the various private and public sources.

State Norms

It is clear that the nation-state constitutes a legitimate authority for Internet regulation. The modalities for the development of the norm are meticulously described in the texts and procedures surrounding this development, thereby guaranteeing a democratic discussion. Application of the norm is granted to 'professional' jurisdictions, surrounded by guarantees of independence and contradictory function.

With regard to 'electronic environments',[24] we may observe two distinct tendencies in state law. One is a preference for notions of variable content, called standards, and the other the entrusting of the interpretation of these standards to relay bodies, sometimes qualified as independent administrative authorities. If we take the Belgian model as a simple example, insofar as the other Western European countries have similar institutions, we would point out the creation of multiple institutions, notably as regards: questions of privacy – the Privacy Protection Commission (Commission de Protection de la Vie Privée); regulation of the audiovisual sector – the Higher Audiovisual Council (Conseil Supérieur de l'Audiovisuel) or the Media Council (Mediaraad); and the telecommunications sector – the Belgian Institute of Post and Telecommunications (Institut Belge des Postes et Télécommunications).[25]

The international dimension of information superhighways leads states to search, at the international level, for models with which to develop the law, or for cooperation between the national authorities entrusted with the application of national laws.[26] Whether through international conventions, such as those of UN, UIT, WTO, WIPO and OECD, or bodies such as the G7 or at the level of treaties for

police cooperation between those engaged in the fight against cybercrime (as illustrated by the draft of an International Internet Charter presented by France to the OECD), a number of public initiatives have been taken to maintain the state's role in the protection and safeguarding both of individual rights and of the overriding public interest. Some[27] go so far as to suggest the creation of an 'International Cyberspace Authority' as a reaction to movements for the emancipation of Internet law and in the face of the increasing power of private norms – an issue we shall now discuss. Global Business Dialogue promoted by the European Commissioner, Martin Bangemann, stresses the importance of setting up this global authority and fixing global rules for electronic commerce.

Private Norms

Contracts The interactivity of networks gives the consent of the Internet's user unprecedented implications. Whether to say 'yes' or 'no' to a 'cookie', to agree to a particular process, to reveal his or her identity or not, to object to non-solicited correspondence – whatever the issue, technology renders the internaut responsible for his or her actions.[28] Tempted by the contractual paradigm inherent in the Internet environment, some authors consider that the state's responsibility to regulate behaviour has been usurped by the substitute responsibility of the citizen, who by his or her consent chooses to authorize or forbid this or that operation.

The principles of autonomous will and the law of covenant, unanimously recognized in every jurisprudence, gives this approach considerable weight, founded as it is on the responsibility of the individual internaut. The contractual approach evidently requires that the technology permit such choices, hence the questions: 'Does the Internaut wish to be identified?' 'For what finalities?' 'Within what time limit?' The internaut must be the object of onscreen choice pages, and the system's configuration must guarantee the respect of such choices.

Self-regulation Trudel defines this as 'norms voluntarily developed and accepted by those who take part in an activity'.[29] We are familiar with the proliferation of such codes, sometimes drawn up locally in a university or in a newsgroup, sometimes on a larger scale for a direct marketing sector or even for the broad mass of activities on the net (such as national charters). The Internet Society, a purely private organization entrusted with ensuring international cooperation and coordination in technology and programming for the Internet, publishes directive guidelines for Internet and network use. In the words of its president:

> It is no longer adequate to base guidelines for conduct purely on the basis of who pays for the underlying network or computer systems resources. Even if that was once sensible, the diversity of constituents of the Internet makes it a poor basis for formulating policy. Thus guidelines for conduct have to be constructed and motivated in part on the basis of self-interest. Many of the suggestions [herein] are based on the theory that enlightened self-interest can inform and influence choices of behavior.[30]

The justification for this galloping self-regulation is a triple one. The argument concerning the technical and evolutionary nature of the object with which this self-regulation is designed to cope is joined by the argument that only the authors themselves are capable of perceiving the risks involved in particular solutions or, more importantly still, of assessing the adequacy and effectiveness of sanctions. The immediate blockade by access providers of a site that has been denounced via a hotline mechanism constitutes a more appropriate and effective response to a pornographic site than any judicial condemnation.[31] The possibility of their development and expansion at a global level serves as a supplementary argument, at a time when the global dimension of cyber-highway problems is uncontested.

Beyond the establishment of norms, self-regulation claims to offer models for applying these norms in virtual communities, as distinct from spatial communities localized in a given territory and subject to national legislation. For some time now we have been aware of the role played by network 'moderators', of the first experiences of 'cybermagistrates' and of virtual tribunals charged with resolving litigious issues in the virtual world. The creation of councils charged with the application of Internet charters represents another demonstration of self-regulation's aptitude not only to develop a supple system of law for cyberspace, but also to sanction it.[32] There is a considerable temptation to see self-regulation as more than just a source of law complementary to that of the state, but rather as a replacement for the latter[33] or, in any case, as a means of dispensing the state from an intrusive regulation. This means that sometimes the private norm will take the place of legislation: for example, the manner in which the delicate question of the attribution of Internet domain names is currently dealt with certainly makes a good case for the integrity and sufficiency of self-regulatory solutions.[34] In other cases – and the current debate between the US administration and the EU authorities about the 'safe harbour' privacy principles is a good example – the adoption of a code of conduct or some other self-regulatory instrument, even if it is promoted or simply requested by the public authorities, will help to avoid the setting up of an intricate administrative and regulatory system which is not considered useful. Further to the entry into effect (25 October 1998) of the European Directive on

the protection of personal data (95/46/EC), the European Commission and the United States (US) Department of Commerce have been involved in a dialogue with a view to establishing a legal framework for the transfer of personal data to the US. It has led the US Department of Commerce to publish the 'Safe Harbour' privacy principles on 15 and 16 November 1999. If the European Commission found these principles acceptable, a decision (under article 25.6 of the data protection directive) could be issued recognising them, as providing adequate protection for the transfer of personal data from the EU to the US.

Certification In a global environment where the network represents the sole means of communication, the definition of certification as a procedure by which a third party guarantees the specific quality of a person or product seems a happy solution.

The aim of certification is to assure the internaut first of the existence and address of his interlocutor and, second, of the other's professional status (see 'Signatures in all their forms', pp.149–52, concerning the electronic signature). There then arise questions of conformity of the other's products to this or that norm, of his or her processes to this or that privacy legislation, of his or her practices to required consumer protection standards and, finally, of the general security of sites. All such problems can be the object either of specific certificates (as, for example, the label delivered by the Internet Consumer Protection Agency (ICPA) or by Trust-e, which deal solely with questions of conformity to privacy standards) or of certification of a more global nature (such as the 'Webtrust' initiative developed by the Association of American Accountants).

Certification presents a solution that may complement either a state normative source or self-regulation, inasmuch as it refers either to a law or to a code of good conduct. Essentially it is based simultaneously, on the one hand, on the quality of the certifying authority and its verification procedures (namely, its independence and expertise) and, on the other, on the effective responsibility of that authority in the event of the unwarranted issue of a certificate. Finally, certification permits easy and effective sanctioning, inasmuch as the company or individual fears the loss of certification and the negative publicity that this would entail.[35]

Practice and the lex electronica Beyond the codified and well identified sources we have so far referred to, we must also deal with principles, whether or not they are more diffuse, which are to be found in the 'Acceptable Use Policies' proposed by Internet access providers, the servers. This 'netiquette' is a sort of 'Ten Commandments' or highway code of fundamental rules for Internet surfers:[36]

1. You shall not use a computer to harm another person.
2. You shall not interfere with another's work.
3. You shall not ferret about in another's files.
4. You shall not use a computer to steal.
5. You shall not use a computer to bear false witness.
6. You shall not use or copy a program for which you have not paid.
7. You shall not use the resources of another's computer without authorization.
8. You shall not misappropriate another's intellectual creation.
9. You shall envisage the social consequences of the program you are writing.
10. You shall use the computer in a manner which shows consideration and respect.

When these rules are contravened, sanctions can take the form of an organized or individual reaction: 'flaming', the disconnection of an indelicate user, the threat of contacting the police and so forth.

The comparison between such practices, spontaneously developed by virtual communities, and the rules of conduct habitually practised by trading communities, gives the impression that *lex electronica* is close to *lex mercatoria*.[37] The similarity is all the more seductive when some authors[38] denounce the dominant economic debate as one which would 'lead to the submission of the information society in general, and the activities of the Internet in particular, solely to the laws of the international marketplace'.[39]

This parallel tends to lend authority to the reflections which now follow on the role of state law in the face of diverse regulatory techniques.

The Role of National Legislation in the Reception and Promotion of 'Private' Sources of Cyberspace Law

Trudel, paraphrasing an observation by Perritt, wrote:

> The parties engaged in international transactions, for example, have developed law-creating practices. Interesting parallels can be drawn here with regard to the regulation of electronic-commercial environments, even though we cannot currently speak of the emergence of a genuine corpus of generally applicable rules. The future of this process of normalization will be favored by the development of more general practices of international arbitration, carried through without regard to differing national legislations. Even if the customs and practices of a given field of activity are often taken into account and, to a certain degree, integrated into national legislation, the nub of such a

> norm still rests in its capacity to autonomously organize behavior and transactions among the members of a community. Respect of these customs and practices is, under certain circumstances, an essential prerequisite for a participant's admission to a given community. Certainly, if the importance of the community justifies it, these customs and practices can constitute a complete regulatory technique, parallel to national legislation, regulating the relationships of members of a community and administered by their own authorities. The model of lex mercatoria from the middle ages is frequently cited as an example. Several current debates are involved with the opportunity of developing a similar legal framework for the regulation of cyberspace; this issue will be analyzed here.[40]

This doctrinal reflection on *lex mercatoria* has led a number of authors[41] to see in it the opportunity for a clear and indisputable recognition of our essential legal pluralism. Developing this idea, Rigaux writes:

> The citizen of a State may possess goods in, or reside in, another State, adhere to an organized religious confession, be a member of a transnational professional organization. The law of each of the States to which he is subject, the law of the church to which he is affiliated, the contractual engagements to which he subscribes in the exercise of his individual economic rights, these all present a variety of distinct legal authorities, each one but imperfectly suited to the others.[42]

From this perspective, self-regulatory acts and, more generally, those private sources of legislation that some choose to refer to as 'soft' law, seem in fact to be legal systems in the full sense of the term, even though their creation may seem less legitimate than a more traditional public process of enactment.

In other respects, without being naive, we must realize that such a system of regulation by the parties themselves is far from being gratuitous. Operators are concerned by such measures either to sidestep national legislations or to subject them to a 'soft' interpretation, yet notably avoid the levelling of grave accusations. The debate on Internet pornography arising from certain recent events, and the resultant proliferation of self-regulatory measures in this respect, well illustrates the argument.

The 'Reception' Given Private Sources by State Law

The three laws: contract, fair trade and responsibility The general and universal principles of national law – particularly those of contractual autonomy, fair and equitable trade and responsibility – can be taken initially as a control model for private sources of 'cyber-law'.

In that context, the different targets pursued by the authors of a code of conduct should be emphasized. Traditionally, the sole target of self-regulation was to fix the rules of behaviour between the actors, authors or those represented in the process of setting up the code of conduct. The main aim, then, is to avoid unfair, uncontrolled competition between them. Sometimes, the code of conduct will pursue another goal and provide solutions with external effects outside the circle of the natural addressees of the code – the authors or representatives of the actors concerned by it. So, when the self-regulation defines the professional behaviour acceptable *vis-à-vis* third parties concerned by the operations regulated by the code of conduct, it is clear that the code of conduct is intended to have effects *vis-à-vis* third parties, including in particular, but not only, parties contracting with the actors submitted to the code of conduct. To take an example, if a direct marketing association forbids or, on the contrary, accepts certain advertising methods or messages, its attitude might affect the third parties independently of the fact that they will become contractual parties. From the legal point of view, this external effect of the code of conduct is more questionable than the internal effects.

As regards the external opposability of the code of conduct to persons who are not only third parties but will become contracting parties and, in that quality, will be considered as submitted to the content of the code of conduct, it would doubtless be sufficient for a judge to go 'to the limits of contractual logic', as Vivant[43] assures us, to become aware of the absence of fully free and informed consent on the part of the internaut in accepting a 'policy' or a code of conduct that barely respects his or her interests. This approach places a question mark not only over the content of the private norm, its conformity with the legal rules, its clarity and its possible unfair character, but also over the integration of the code of conduct within the scope of the contract, which might be questionable when the code of conduct is referred to only by a hyperlink that is difficult to activate.

The other 'third parties' might consider themselves prejudiced by a behaviour which, although in strict conformity with the content of the code, has recourse to standards such as 'good faith' and *in pater familias* – those 'as well as possible' forms often permit lip service to be paid to the adoption of an ethical code, respectful of its norms of prudence and diligence and its sanctioning of violations of a norm developed by a private judicial system, to the degree to which that norm represents a professional standard whose contravention automatically constitutes a fault.[44] However, recourse to standards authorizes the denunciation of self-regulation or systems of certification whose content does not seem to respect those standards.

The adoption by one faction of 'codes of conduct' or of 'technical norms' may be intended to prejudice the competition in some way. It

will be sufficient to invoke the principles of free and fair trade to strip them of all value.

Rejection of private judicial systems where public order has been contravened The body of jurisprudence dealing with the activities of associative authorities, both at the time of enactment of disciplinary rules and during their application, permits us to extrapolate certain rules which are relevant when tackling the subject of self-regulation in cyberspace. This applies equally to legal systems whose right to create norms is undisputed. While not contesting the autonomy of the norms enacted by a given profession, jurisprudence has sometimes nonetheless called them into question, particularly in situations when the professional norm is in conflict with a state norm judged to be in the public interest.[45] So, for example, if a code of conduct authorizes a server to process data obtained by means of cookies, without prior information of the Internaut concerned, it would constitute an infringement of the principle of transparency upheld by the data protection directive. Furthermore, the space available for self-regulation is reduced each time a conflict involves a superior motive or fundamental value. State law will either by decree or recognition proclaim such norms as being in the public interest. This assertion should, however, be nuanced by the following consideration: the efficacy of the state norm can be reduced insofar as state authority does not possess the means to enforce it. In such a hypothesis, the state recognized norm is granted a value more symbolic than real, and self-regulation may represent the lesser evil.

Jurisprudence has also sometimes questioned professional norms in situations when the application of the norm represents an abuse of rights inasmuch as the sanction is disproportionate to the infraction concerned, or its levying has not taken into account the minimum right to defence according with Article 6 of the European Convention of Human Rights. This question is delicate in so far as the self-regulation pretends to external effects particularly when privacy or consumer protection questions are addressed by the code of conduct or by technical norms. One would like to underline the very interesting solution foreseen by Article 17 of the draft proposal of the Directive on certain legal aspects of the electronic commerce: 'Member States shall ensure that the bodies responsible for out-of-court settlements of consumers apply the principles of independence and transparency, the adversarial principle, and the principles of effectiveness of the procedure, legality of the decisions, liberty of parties and representation.

In an Internet context there are certainly instances of sanctions which, through their unilateral application by less than transparent authorities without any external control, may be deemed abusive of a party's rights. Thus the immediate revoking of a server's certificate

for alleged behavioural non-conformity to a code of conduct may seem to be an unacceptable censure to a state authority concerned with the respect of freedom of expression and the principle of unrestricted defence.

The Promotion of the Private Legal Authority: Reflections on the 95/46 Data Protection Directive

Two types of promotion Taking as a departure two provisions of the Directive referred to, we should like to show:

- with reference to Article 27, how state law articulates both public and private norms and thereby promotes the adoption of the latter
- with reference to Article 25, how a national legal authority, while respecting the culture and system of other legal authorities, can establish certain criteria for the recognition of private norms conceived in those other legal authorities.

'Monitored codes of conduct' Article 27, paragraph 1 of the Directive affirms that the Commission's member states 'encourage' the enunciation of codes of conduct destined to contribute – depending on the specific nature of the sectors concerned – to the correct application of national provisions. The editors of such codes can submit them to monitoring authorities that would verify their conformity with existing regulations. The text also envisages the drawing up of community codes for submission to a European data protection group which would examine their respect for national provisions.

Once the codes have been submitted for their inspection, both the national monitoring authority and the European group can, 'should they deem it appropriate', gather the opinions of the persons concerned or their representatives. Finally, depending on whether the code is national or European, each of these authorities respectively can take steps to ensure publication.[46]

The principle enacted by the Directive is a simple one: both self-regulation and certification systems represent effective tools for the enactment of the provisions laid down in the Directive. They contribute to the improvement of the brand image of those who submit to them and increase the confidence of the internaut. Their flexibility and specificity make them suitable tenders for evolutionary solutions adapted to the particularities of each sector. Finally, their European character serves to guarantee equivalence of protection with regard to electronic processes operating in any corner of the continent.

Recognition by state authorities of these codes of conduct takes two forms. The formal procedure of confirmation does not only apply

to the basic criteria which constitute respect for the provisions of the directive, but also to more procedural criteria: the publishing of the content of self-regulation or criteria for certification, the transparency and openness of debates, taking into account the range of parties interested in these processes, in particular those directly concerned.

In any event, the codes of good conduct cannot exempt the server from applicable areas of national legislation derived from the directive which guarantee, admittedly in general terms, the respect of subjective rights and the possibility of appeal to justice for the persons concerned. Such submission to the law brings to codes of otherwise restricted range, if only indirectly, a certain legal weight, given the fact that the law, accompanied by the restraining force of justice, remains the ultimate guarantee of the effectiveness of the principles enunciated therein.

The European Council Recommendation of 24 September 1998 'on the development of the competitiveness of the European audiovisual and information services by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity'[47] goes further. A number of indicative guidelines, aimed at ensuring the full participation of all interested parties (public authorities, consumers, users and industries) in the drafting, implementation, evaluation and control of the respect of the codes of conduct, are annexed to it. This participation is regarded as necessary in order to legitimate the recourse to self-regulatory solutions.

The amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market establishes, in the same way, that 'In so far as they may be concerned, consumer associations shall be involved in the drafting and implementation of codes of conduct. Moreover, the actors must ensure their complete transparency and accessibility including as regards their evaluation.'[48]

'Adequate' protection, or how a state authority can impose its values in a flexible manner on a third country in the global information society By virtue of Article 25.1 of the Directive:

> ... the Member States stipulate that, in the event of a transfer to a third country of personal data as the object of a process, or intended to be subjected to a process after transmission, such a transfer may not take place unless, subject to national provisions taken in application of other provisions of the present directive, the third country in question can assure an adequate degree of protection.

The principle is therefore to prohibit transmission unless the third country can prove an adequate level of protection.

The Directive, rendering this yet more precise in Article 25.2, goes on to say that an evaluation of the adequate nature of data protection in a third country must take into account 'all circumstances relating to a transfer or type of transfer' and in particular the different factors, of which some are integral to the type of transfer being considered, such as the nature of the data itself, the finality and the duration of the process, the country of origin and the country of destination, and others concerning the level of protection in the third country such as 'current legal provisions both general and sectorial, as well as professional rules and the security measures which are respected there'.

In particular, the text of Article 25 presumes a functional approach – that is, that protection should be evaluated as much according to the risk of attack on the data's protection and risk arising from the type of flow in question, as according to the specific or general measures undertaken by the party responsible for the data in the third country to reduce such risks.

The evaluation of these measures should be made without *a priori* judgement. There is no question here of imposing European mechanisms developed in response to the Directive on a third country (that is, there is no European imperialism), but rather of appreciating to what degree the goals of protection pursued by the Directive are encountered there, whether in an original way or not. In this sense, the idea of adequate protection does not in any sense represent a weakening of that data protection envisaged by the Directive. In effect, the idea of adequate protection induces a confrontation between the protective demands of the Directive and the responses given to these by the third country. The aim is to ascertain whether there is a 'functional similarity'. Such a 'functional similarity' implies that we are concerned to find not a pure and simple transposition of European principles and systems of protection in the third country, but rather the presence of those elements fulfilling the required functions, even if the said elements are of a different character to those with which we are familiar in Europe. This certainly encourages a better respect for local structures and legal characteristics than would the requirement of equivalent protection, which calls for complete legislative similarity.

In particular, with regard to the protective instruments installed in the third country, Article 25 not only refers to norms established by public authority, whether general or sectorial in character, but equally to codes of conduct or technical measures, provided that these are 'respected'. Thus the person entrusted with evaluating foreign protection would be more attentive to the 'effectiveness' of an instrument than to its nature: what matters is that knowledge of the instrument in question – even if it is just a simple company privacy policy – be

widespread among the persons concerned and among those responsible for files; similarly the trustee would be mindful of the option of claims or appeal by individuals calling those responsible to account in the event of any act of non-respect for these instruments. Finally, he or she would meticulously evaluate the quality of the authority in charge of claims and appeals, its accessibility and its functional transparence.[49]

Conditions of self-regulation What conclusions can we draw from these two provisions of the Data Protection Directive to serve as lessons both as to the value of private norms and to the synergy between these and the norms established by the state?

First, the private norm is the better accepted for being defined within the framework of principles or standards established by the state norm. Such standards not only enable an evaluation of the private norm's conformity of content to society's expectations, but also assure it greater effectiveness.

Second, the private norm may be deemed 'adequate' as compared to the state norm if the procedure under which it was drawn up conforms to certain demands of legitimacy: first, the degree to which that procedure has permitted the expression of the opinions of, and taken into consideration the interests of, the different parties concerned by the operations to be regulated; second, the transparency of the norm in question; and, finally and most importantly, whether it is genuinely effective – that is, that binding sanctions can be handed down by an authority equipped with powers of investigation, acting independently of the parties concerned, easily accessible to all and whose dealings are transparent (for example, via a public report of its activities or the publication of its decisions).

Some Conclusions

The state norm: a necessary intervention With regard to state sources, what is the use of a national legislature legislating when, as we have shown, first, the international character of the network and, second, the impossibility of mastering the space–time coordinates of exchanges, lead us to admit the impotence of nation-states in the effective application of the norms which they have drawn up? The emotion's aroused in 1996 by the intervention of a German court, charging access servers with having allowed pornographic material to filter through, shows, however, that even if state law does not have completely effective instruments at its disposal, it is nonetheless capable of motivating private parties to put self-regulatory solutions in place which are at least partially, if not totally, satisfactory. The state, therefore, cannot simply resign; instead, without pretending to efficiently

police the network, it should duly call attention to the social values that enshrine the norms, even if this is only to provoke appropriate self-regulatory reflexes and to serve as their basis. It is quite noticeable that even in the United States – the country which is deemed to be the leader in the defence of the self-regulatory solutions – public bodies are playing an ever greater role in promoting, or even requesting, these solutions. Thus, Mr Pitofsky, Chairman of the Federal Trade Commission, asserted in August 1998: 'Unless Industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional government authority will be appropriate and necessary.' Since this statement before Congress, the US Government has taken different initiatives such as the 'Global Alliance' in order to protect privacy effectively in the context of its discussion with the European Union in the matter of Article 25 of the Data Protection Directive.

Furthermore, the search within supranational bodies, such as UNESCO, for common principles and solutions in areas such as the protection of minors, consumers, the electronic signature and so on, favour the normalizing of working channels and, indeed, of cooperation between states (even if only among police forces). In the absence of such a consensus, the position taken by a supranational organization such as the European Union can serve as a departure point for international negotiation with other countries also entrusted with the search – doubtless via means more in keeping with their own legal traditions – for adequate protection *vis-à-vis* the principles enunciated by the European Union.

Confronted with the social revolution that the Internet represents – particularly in terms of the dislocation of space–time frontiers – state law, as the expression of the social regulation of behaviour, is, and has a right to remain, present. The law cannot allow itself to be content with deploring the limitations placed on its own enforcement and affirming the essential lawlessness of cyberspace. On the contrary, it must find, in the context of a pluralist normative expression, an adequate active role. As far as possible it will refer, by application, adaptation or reform of general principles, to the normative mechanisms present in the network: the application of principles via self-regulation and technical standardization. Depending on the case, it will draw its inspiration for the defining of rules of law, if possible at the international level, from the content of internal network regulation. What we are seeing here, to use Vivant's expression,[50] is without doubt the emergence of postmodern law, or what Reidenberg refers to as a new 'network governance paradigm'.[51]

Far from sanctioning the state's resignation, this 'postmodern law' – this new 'paradigm' – calls for the creation of new forms of dialogue

both between diverse ethical and regulatory normative techniques and, more problematically, between the democratic authorities capable of nurturing such a dialogue and placing it at the service of the public interest.

On the one hand, the state cannot abandon Internet regulation to the sole initiative of its users. We have seen clearly that, in the absence of specific regulations, a reaffirmation of major legal principles spurs the parties to take measures and leads to the development of appropriate techniques. On the other hand, we should like to stress the state's vital obligation to intervene at a time when, in our opinion, deserting the Internet and withdrawing from the field of regulation to such a point that it no longer even decides the general framework, would notably put at risk public order, fundamental liberties and other basic values.

The precise division of labour between the drawing up of state or supranational law and the regulatory initiatives of Internet users remains to be defined. It will doubtless be a dynamic relationship, and one that must enable the users to demonstrate a certain creativity in the enactment of the framework proposed by national legislation.

The value and limitations of self-regulation This said, there can be no question of rejecting self-regulation as a normative source in the fullest sense of the term. As Osman concluded, 'whether we choose to see in this uniquely "a question of time and context" or the proof that the law must "progressively suffer both the attraction and the yoke of the economic facts" which dominate it and to which it has become a tributary',[52] such a phenomenon can only serve to awaken the interest of jurists who have been taught that the sanction is part of the mechanism of the rule of law. Naturally they are tempted to search everywhere, even in 'soft' law. And if the criterion of the sanction as a 'characteristic of the rule of law is a false [one], despite doctrinal attempts to revive it, this is doubtless because the effectiveness of rules of social conduct, whether they "rule or regulate", does not necessarily reside in the adherence to them by the social body for which they are destined'.[53]

This reflection, which addresses the normative sources of *lex mercatoria*, certainly ought to be equally applicable to *lex electronica* but it cannot have the same range, and this, without doubt, justifies a more resolute intervention on the part of state law. First, the Internet environment, except in the newsgroup context, or in certain contexts, such as universities or trade between merchants, does not have anything like the same homogeneity as the professional environment. Second, whereas *lex mercatoria* only regulates economic questions, *lex electronica* is concerned with culture, values and liberties.

It would seem, therefore, that self-regulation should be controlled. Although it is certainly capable of representing the spontaneous expression of a particular community, this is rarely the case. Furthermore, state law is obliged at least to fix the standards which serve as a basis for the development of self-regulation and its associated normative techniques and to ensure that the mechanisms for the setting up of these regulatory techniques and the application of the content of these private norms is transparent and takes into account the interests of the various parties concerned.

THE ROLE OF THE STATE AND THE DEFENCE OF VALUES

Traditionally the role of the state is defined as being threefold in that it consists of regulation, stimulation and production. The function of production is understood as the development of goods and services. In the information society, this function tends to be whittled down, such is the degree to which the merits of free and fair competition and the financial needs of the state have led the latter to separate itself from the entities of production, particularly in the telecommunications sector in which the state formerly enjoyed a monopoly, but also in the general exploitation of telematics administrative services (such as multimedia data banks on the subject of ratable property values) where the state increasingly relies on outsourcing.

The stimulatory or catalytic function can take place in a variety of ways. In the same way that adequate regulation, including fiscal policy, can be a useful lever for the development of computerized goods and services, the transformation of processes within the government, or between the government and the people, via the introduction of information and communication technology, can lead to the people adopting that same technology. It is for this reason that all national programmes relative to the information society speak of the need for a 're-engineering' of public functions, and it is a fact that the use of electronic forms for administrative purposes, such as value added tax (VAT), is leading companies increasingly to expect electronic invoicing from their business partners.

The first function of regulation constrains the state to espouse the cause of liberty. Indeed, the earlier discussion not only stressed the complexity of the legal debates arising from the use of information and communication technologies, it also bore witness to the recurrence and omnipresence of the issue of liberties.

The following reflections derive from the recognized fact that the increasingly significant incursions of economic operators, supported in their activities by recent developments in the safeguarding of electronic messages, are radically reshaping the landscape. As stated

earlier, the Internet is rapidly leaving the 'forum of ideas' which characterized exchanges within the scientific community where the Net was originally conceived, to enter the world of the 'trade fair'. Thus two worlds currently appear to exist side by side within the Internet:

> The first being cyberspace, close to the 'forum of ideas', where technology appears, on the one hand, to be a mode of expression – some would say 'free' – of each and everyone, an expression all the more free for the fact that the author of a message can decide whether or not to identify him or herself and choose the correspondents with whom he or she wishes to communicate and, on the other hand, a means of access to the free creations of others, wherever they may be in the world;
>
> The second being the 'superhighway', not unlike a 'trade fair', where technology appears as an extraordinary tool at the service of the market, enabling it to improve information production circuits, but above all to control distribution. Electronic services for copyright management and the creation of centres for the certification of messages (see Part I above) are best understood in this light.[54]

In other words, the Internet's development oscillates between two worlds: one of uncontrolled ideas and the other founded on the laws of the marketplace and the rules of property.[55] And it is in taking this revolution into account that we confirm the essential role of law and regulatory functions in maintaining a free society.

Regulatory function can be understood, in one sense, to mean drawing up the rules of the global game – rules that are valid for a given society, either general (as for example, the laws of fair trade) or specific to a particular sector (such as audiovisual law) – or, in another sense, applying those rules by means of 'new regulatory bodies', those 'independent administrative authorities' whose existence and proliferation have already been indicated (see pp.152–5 above).

Shorn of its productive function, the state concentrates its role around the defence or, preferably, the promotion of certain values. Thus even such a privatistic issue as that of contractual law nonetheless raises challenges to questions of liberties and non-discrimination. This is the case with the appearance of 'electronic notaries' and the right of every person to an electronic signature. It is the case with the need to develop, for reasons of privacy protection, the right to the use of anonymization techniques for transactions, whether towards certain parties to the transmission or the recipient. It is the case in the laws of intellectual property, as expressed in the idea of obligatory licensing, when the desire emerges not to reserve the right of information access solely to the 'haves' of this world but to guarantee it to all, if we are to avoid a two-track society. Finally it is the omnipresence

of the principle of freedom of expression which, as the jurisprudence of the European Court of Human Rights reminds us, cannot be limited by superior interests and liberties except in so far as such limitation is strictly necessary for the protection of these selfsame interests and liberties, which leads the state, not only to avoid any excessive regulation, but equally to take care that self-regulation does not become a more insidious and effective tool of censure than any police surveillance could be.

Beyond this, the state will endeavour, on the one hand, by a policy called 'universal service', to ensure that each citizen enjoys the possibility of access to the benefits of the information society and, on the other, to introduce appropriate instruments to ensure a better participation of all citizens in defining the *res publica*, by avoiding the traps of what some call 'electronic democracy'. It is these last two points that will be addressed below.

Beyond the Universal Telecommunications Service: The 'Universal Service' in the Information Society

The Universal Telecommunications Service

The proposal to create a universal telecommunications service is based on an indication that the citizens of the information society demand more than that defined by the European Union following the reform of autonomous public services. The concept is defined as a service that is universal (providing access for all at a reasonable price), equal (implying non-discriminatory access quite independent of geography), and continuous (characterized by uninterrupted service of a given quality).

The concept of a universal service has the merit, while respecting the dynamism of a competitive market and therefore refusing all state monopoly, of accentuating the manner in which new technologies should permit everyone to better participate in society and in the definition of the collective will to co-exist. In this respect, the expansion of the universal service concept is evolutionary in so far as it takes into account technological developments and their increasing distribution within society.

The universal service is initially understood as access to communications technologies: to the network or today's telephone service, to e-mail and to the information superhighway of tomorrow. Until now, only this universal telecommunications service has been considered by European texts.

A second aspect of the universal telecommunications service, already present in certain European countries and encouraged by

Belgian legislation of 17 December 1997, favours the connection of schools and public libraries so that everyone may have access to technological culture.

The Universal Service in the Information Society

President Clinton and Vice-President Gore's 'National Information Infrastructure Policy' (1993) has brought a revolutionary dimension to the concept of a universal service, without much altering its definition. The universal service concept grows daily in vitality and represents a means of fighting against social discrimination.

That political will was enshrined in the Telecommunications Act (1996), section 254 of which establishes the principles of a universal service, defines its expansion and, finally, establishes a periodic revision procedure for its contents.[56]

The consequences of such a positive approach, which founds the development of an information society upon the flowering of our liberties, highlights the importance – even necessity – of a redefinition of the universal service, no longer understood only as the access to technical means of communication (infrastructure and voice transport service), but equally as the means whereby the demands of creation and provision can be introduced openly into the concept of universal service, as that which is considered 'essential' and 'vital' for assuring the people's participation in a democratic society. The task here, according to the American policy definition given in the 'National Information Infrastructure Policy' is to take care that no discrimination occurs between those with the necessary know-how and those without – the information 'haves' and 'have nots'. As proclaimed by Principle No. 1 of the UNESCO Experts Group (1998), 'The right of communication is a fundamental human right' and, therefore, 'Every citizen should have the right to meaningful participation in the information society' (Principle No. 2). This implies that 'States should promote universal services where, to the extent possible given the different national and regional circumstances and resources, the new media shall be accessible at community level by all individuals, on a non-discriminatory basis regardless of geographic location' (Principle No. 3).

Even if multiple and various expressions of this right have to be realized according to the level of development of each country, the issue is not merely one of ensuring technical access to a network or service, at a reasonable price and in a non-discriminatory manner, but of giving access to the information content itself. We are already familiar with certain well known examples in the United States, such as access to training and health care. The important thing now is to make certain services of public interest available to everyone by

means of telecommunications systems of different parameters according to the type of service, if there is not to be a two-tiered society.

To this end, several national reports (Canadian, Danish, Dutch and French, *inter alia*) stress the need for a voluntarist education policy in the use of these technologies in secondary and even primary schools. Apart from the actual linking of schools to the infrastructures, the use of interactive technologies can be a valuable teaching aid, while at the same time encouraging students to master the new technology. Such an educative process should also include lessons in the reading of onscreen images, whether in the form of advertising, of general information or other, in order that future users of these new media may know how to 'decode' the messages that the network provides. In the words of the UNESCO Experts Group (1998):

> All persons should have a right to appropriate education in order to read, write and work in cyberspace. There should be specific initiatives to educate parents, children, teachers and other Internet users on the implications of their participation in cyberspace and on how to maximize the opportunities presented by the new media. (Principle No. 6)

In addition there is an interest in the creation of 'information centres' open to everyone in locations such as public libraries. Local experiments attest to the dual benefit of such centres: first, they enable populations which, for financial reasons, have difficulty in accessing electronic information services to come online at a reasonable cost; second, they stimulate direct contact between individuals grouped around a terminal and thereby diminish the risk of an 'isolating' technology, where only virtual, individualistic communication is on offer.

On the medical front, the concept of a Universal Public Health Service is being developed – in other words, a positive commitment on behalf of the government to establish online assistance services to help with the filling out of forms, and medical information services for statistical and other purposes. This is, in its turn, the source of the state's duty to subsidize certain establishments, notably in higher education, for access to, and diffusion of, such data.

Under the heading of a Universal Public Health Service is also found the creation of information infrastructures of high capacity and output between hospitals situated in low population areas with few highly qualified staff and hospitals which, either due to their geographical position or to their university status, employ highly qualified personnel. Such networks serve to improve the standard of the health service.

This strategy can be extended to other sectors; in many fields of governance, information technology could improve citizens' access

to public services, whether to the social services, or for the issuing of building permits, or access to the fiscal authority, or helpline services for the filling out or sending of administrative forms, or to the public services of the judiciary for the electronic certification of messages, the lodging of complaints or the deposition or exchange of findings.

Basically, the entire functioning of a government and its attendant services can be reviewed in the light of its potential for the development of information and communications technologies.

This transformation of government services has its legal foundation in the law of mutability – a key principle of public service – and in the laws of access to government documents. Particularly in an electronic environment, this right should be understood not only in terms of ensuring citizens' right to be informed by their government (see the following section) but, in a more voluntarist context, in terms of the government's desire to be of greater service to its citizens.

The recent national legislation regarding the electronic diffusion, particularly via the Internet, of the various public regulations and court cases are an example of this.[57] But above and beyond this, the possibility for a citizen to follow the progress of his or her application for a building permit, for instance, and be further able, thanks to a decision helpline system, to understand the logic of the regulations involved in that permission, constitute even more remarkable advances in the application of the citizen's right to administrative transparency.

The Virtues of a Large Concept

To conclude, the virtue of a universal service concept is a multiple one. First, a social goal is being pursued by those advancing the concept: a dualization of society is to be avoided. Second, the necessarily evolutionary content of such a universal service calls for forum discussions by all parties involved before the public authority makes any decision, and is thus a gauge of the participation of all in defining the information society of tomorrow. Third, the concept of a universal service, in preference to a simple public service, accentuates the possibility of private sector participation in one or other of the tasks of setting up or distribution of each service deemed to be of public interest. This collaboration between government and the private sector may be seen as a better guarantee for the effectiveness of the service, provided that a private monopoly is not substituted for a public one, and that guarantees to this effect exist in the form of laws of competition, public markets and so forth.

Electronic Democracy: From Myth to Reality[58]

Technologies of Information and Communication and Democracy: A Multifaceted Dialogue

The new information and communication technologies are equally capable of promoting freedom of expression and information and, in a wider sense, democracy. They facilitate a citizens' access to public information, offer them the possibility of being consulted or of intervening more directly in the decision-making process, and can even pose a danger when used to dubious ends by political parties or lobbies wishing to influence a political decision.

Two questions relating to these themes shall be examined here. First, reflection on the subject of information superhighways is stimulating a revitalization of the laws of access to government files (Freedom of Information Acts). Thanks to the administrative transparency that these laws assure, they emerge as an indispensable prerequisite to citizens' free and informed expression of views in a democratic society. Second, these same technologies offer citizens the possibility of being consulted or of intervening more directly in all decision-making processes, particularly at the local level. This will lead to increased use by political parties of the facilities offered by the new technologies, thereby raising not only hopes, but also such fears as to justify defining certain rules of the game.

From Access to Administrative Documents to Electronic Access

The cornerstones of legislation The freedom of expression recognized in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms presumes, if it is to be effective, an obligation on the part of the state which is as much passive as it is active – an obligation to inform both of the action taken and the action intended. The public's right to be informed, understood not as a subjective right but as a democratic principle, finds its primary expression in the freedom of information.

This, bearing as it does on the relationship between the governed and the powers that be, takes on a very particular sense and signifies the ability of every citizen to gain a knowledge of government files as well as information held by public authorities. Freedom of information, the instrument of transparency for public and administrative institutions, offers, through this progress towards the installation of participatory democracy, the indispensable complement to current regimes of representative democracy. The open debate within the body politic cannot take place except on the basis of access to all information held by the public sector.

This assertion has already served as a foundation for the very principle of the Council of Europe's recommendation on access to information held by public authorities, a recommendation which was taken up by numerous national 'freedom of information' laws. The use of information and communication technologies (ICTs) gives new forms – not to say a new significance – to this right of access.

Electronic access to administrative documents Under the impulse of the American 'National Information Infrastructure Policy', simple technologies have been set up all over the United States, particularly at the local level, permitting over-the-counter access for citizens to exercise their rights under this legislation more effectively. In this way citizens can obtain information and services (population or land register, tax service, social security) from the municipality either from a home terminal or from one of the counters at different points in the town.

This is not just a matter of ensuring access to, or distribution of, statistical, geographic, demographic, administrative or legislative government databases, but of permitting an interactive electronic dialogue between the government and its citizens. Hence we can imagine citizens, thanks to the interactivity of these networks, being able to question their governments on those procedures which concern them (say, building permits, entries in the commercial register and so on) and to accomplish this without needing to leave their homes. This means that the people can continuously monitor documents which concern them.

By pushing this reasoning still further, it might be asked whether the processing of administrative data should not be conceived in such a way as to enable the people to access the process itself directly via their own terminal. These questions are the subject of current discussions in the context of freedom of access to electronic information in the United States, but it is only in Canada, at the federal level, that the law has opened up the right to include 'computer time' – in other words, the duty of public authorities to perform the necessary data programming, as a means of responding, including via electronic means, to each interested citizen requesting direct access.

The evidence of a multiplicity of developments and suggestions indicates the desire for a profound change in the right of access. This is not simply a matter of ensuring citizens' rights to be informed by their government but, thanks to information technologies, of transforming, through a more voluntarist approach, the now transparent administration into a better service for its citizens.

However, these new ICT implementations will raise the problem of accessibility for all citizens to the network. The denial of a two-tier society of 'haves' and 'have-nots' is justified not only for reasons of

ethics or social justice but also in terms of democracy by which everyone is entitled to access administrative and governmental services. The state has a duty to abolish any barriers to such access to these new services. In that context, according to Wellman and Buxton,[59] three levels of accessibility should be distinguished: technical, economic and, most importantly, cultural. The 'physical' or 'technical' aspect is within reach, due to of the spectacular evolution and dissemination of the technologies; the economic aspect will shortly be resolved thanks to the continuing fall in prices, the provision of computers in public libraries and schools, and the development of the universal service concept; the outstanding challenge is the cultural aspect because of literacy problem for certain populations. In so far as the state is unable to ensure these three levels of accessibility, it is duty-bound to maintain traditional means of access to the administration.

Improving Citizens' Participation in Political Decision-making

'Civic networking', virtual towns The interactivity of networks means that they can be regarded as a more sophisticated tool for dialogue between the citizenry, on the one hand, and decision-makers and lobbyists on the other. The Internet already offers numerous 'bulletin board systems' where messages on public-interest matters of local, national or international importance can be exchanged individually or thematically.

Professor Rodota has described the US experiment in this respect as follows:

> In the United States, alongside the Internet experiment and the other big telematics networks, numerous local experiments can be observed, of which the majority are managed by private 'civic networking' organizations. About a hundred American towns are equipped with operational Civic Networks or FreeNets (networks accessible either free or for a nominal fee). To co-ordinate their development they are grouped together in a 'network of networks', the National Public Telecomputing Network (NPTN) which groups all these appropriately called 'Digital Cities' together. These organizations not only provide Internet access, but also link citizens to public offices, libraries, archives, schools, universities, hospitals, research centres and companies. The main aim is to offer users a series of services which deal with government and legislation, administration and politics, as well as with social issues, sanitation, education and economics.[60]

Such services for popular consultation should be organized systematically by governments at every level – local, regional, national and even international – with due observance of the laws of privacy.

What is at issue here is a modern form of organization for public hearings, capable of usefully enlightening decision-makers by informing them of both individual and collective points of view. Certain rules should be followed in order to ensure the transparency of procedure both at the initiation stages and in the results, which should be accessible to both opposition and majority.

The electronic referendum Ross Perot, the ill-starred American presidential candidate, contributed to the popularization of the concept of the 'electronic town hall'. This involves an authority – particularly, though not exclusively, a local one – in the development of electronic modes of decision for its electorate. The aim is to install, alongside representative democracy, a form of direct democracy, enabling more rapid political consultation and offering citizens a way of reappropriating the *res publica*.

This type of electronic referendum experiment favours direct democracy. However, the institution ought to be evaluated, taking account not only of its technical potentialities but also of its implications for our contemporary political systems. While retaining complementarities with the representative version, the electronic referendum nonetheless carries with it risks of derailment accentuated by its 'push-button' aspect.[61] There is clearly a risk of public manipulation inherent in this type of procedure, whether in the choice of problems to be dealt with by referendum or in the phrasing of the questions put to the population. But it is also to be feared that the technology trivializes this type of consultation and that its very interactivity – via the threshold of a screen which creates a sort of 'living-room democracy' – deprives citizens of the necessary guarantee of distance, private reflection and public debate, necessary as much for an understanding of the significance of the question being posed as for reacting to it.[62]

Undoubtedly, ethical and normative rules will need to be enacted to this end. Thus, in any hypothesis, the aim, modalities and consequences of the consultation and the authority responsible for carrying it out will have to be clarified. A prohibition against recording any personal data accruing from polls taken in this way has to be affirmed and, in cases where the electronic consultation is organized by a public authority, the following obligations imposed:

1. Prior to the poll, the questionnaire should be submitted for discussion within the representative democratic bodies and, depending on the case, the remarks of each faction of opinion on the questionnaire should be made publicly accessible.
2. The questionnaire and the reflections upon it should be published both electronically and otherwise, prior to the poll.

Modalities other than the electronic option alone should be provided for.

A complete review of the results of the referendum (in particular the number of persons who voted and the modalities of the poll and so on) should be published.

5. No decision should be based solely on the results of an electronic referendum.

Use by politicians and political parties of information and communications technologies A number of examples testify to the importance of electronic media in the diffusion of party political messages. The *Berlusconi* case is often cited but, far beyond this, we can observe how each party – indeed, each politician with electronic server access – is increasingly organizing the communication of information or provoking debate on this or that subject via electronic systems.

Some authors do not hesitate to denounce the dangers of such a mediatization of the political process, short-circuiting as it does traditional forms of political apprenticeship and engendering a simplification of issues into populist slogans and caricature. Above all, using such media leads to the formation of political opinion outside the common forums (electoral meetings and so forth) where such opinion was traditionally forged.

In the circumstances, we should ensure that school curricula include courses in the critical analysis of messages via the new electronic media. Furthermore, it is vital that access to the new media should be guaranteed for all shades of opinion and that, as in the case of party political messages in the classic press and audiovisual media, similar rules should be drawn up for their operation. These should ensure the proper identification of the nature of such messages and of their authors, access for all citizens via a single terminal to the political messages of all the different parties, and the anonymity of citizens consulting such programs should they so request.

Many electoral rules – those relative to the organization of electoral campaigns, to the laws of defamation and the right of response, to the strict control of electoral advertising, to the prohibition of the publishing of exit polls during the election, to the length of campaigns – are difficult to apply outside the context of the traditional media and 'invite a certain revision of our habitual regulatory thought patterns'. Without this, audiovisual communication law will lose all coherence and shatter into a multitude of specific laws, each relating to an individual medium, and the mechanisms of electronic democracy will be subverted by the capacity of the technology.

CONCLUSION

The role of the law in the face of developments in the information society is a multiple one. Its first mission is certainly one of critical re-evaluation. There is no question of yielding to the temptation of modernity and, by a circumscription both hasty and rough, enshrining in law the originality of technological data. On the contrary, the invitation to 'reread' the law demands a period of distance to enable us to steep ourselves both in the values and balances etched at the heart of traditional concepts and in the need for awareness of the new challenges.

To resolve these new challenges, the jurist's task – and this is his or her second mission – is to become a mediator between the diverse and often conflicting interests that are spawned by the different categories of users of these new technologies. Rather than congealing into law the results of arbitrages – results which will be disputed in the short term – the law has a duty to set up mechanisms with which to measure, quite openly, the degree to which evolution is altering a fragile equilibrium that is hardly definable.

Such a conclusion pleads for a law that is more one of procedure than of content. Open and transparent spaces in which this discussion can take place have to be created. Such spaces are legion. Apart from the public sources, the norm may emanate from private circles. The law needs to recognize such norms and multiply the dialogues between public and private authors, building that 'internormativity' which characterizes the regulation of information and communications technologies. With regard to private sources, the state will remind us, meanwhile, of the demand for legitimacy for their authors and their content – a legitimacy which can only emerge from the transparency of the discussion, or at least from taking into account the interests of each party concerned by the question under debate.

The same concern for flexibility and mediation between parties with divergent interests stimulates the law to swell the ranks of the 'independent administrative authorities', granting them the same creative autonomy while demanding functional transparency and openness from them in return.

Finally, the will to define a 'willingness-to-cohabit' should lead to the creation of a place of national reflection, a place of technological vigil, for the concentration and definition of global policies – a place where, in the course of public debates, the major options of our society will be forged. We will have then created a society not only of information but of democracy.

NOTES

1 The main ideas in this text were initially presented to the Information Society Working Group of the Belgian Royal Academy of Sciences on 20 March 1998. It has been extensively reworked until the end of 1998 in the context of research carried out under the interuniversity 'Poles of Attraction' programme sponsored by, and for, the Federal Department of Scientific, Technical and Cultural Affairs of the Belgian State.

2 See p.170.

3 P. Trudel et al., *Droit du cyberspace*, Montreal: University of Montreal/Editions Themis, 1997.

4 UNESCO, 'Experts Meeting on Cyberspace Law. Working Document', Paris, UNESCO (CII-98/Conf.-601.2), 1998, para. 12.

5 UNESCO, op. cit., para. 10.

6 See Y. Poullet, 'Le droit de l'informatique existe-il?', *Droit de l'informatique: enjeux-nouvelles responsabilités*, Brussels, Conférence du Jeune Barreau, 1993; also J. Reidenberg, 'Governing Networks and Cyberspace Rule-Making, *Emory Law Journal*, 1996, p.911.

7 See C. Lamouline and Y. Poullet, *Des autoroutes de l'information à la démocratie électronique*, Report to the Council of Europe, Brussels: Nemesis/Bruylant, 1997.

8 See S. Gutwirth, 'Waarheidsaanspraken in Recht en Wetenschap, een onderzoek naar de Verhouding tussen Recht en Wetenschap met bizondere illustraties uit het informatierecht, thesis, Maklur, Antwerp, 1993.

9 See M. Antoine and D. Gobert, 'Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification', *Revue Générale de Droit Civile*, 1998, pp.285–310.

10 See Y. Poullet, op. cit., p.17.

11 See Y. Poullet, 'Libertés fondamentales et société de l'information', *Revue Générale*, no. spécial, *Communication ou a-communication*, March 1999, pp.21–8.

12 See S. Dussollier, 'Electrifying the Fence: The Legal Protection of Technological Measures for Protecting Copyright', *European Intellectual Property Review*, 1999, pp.285–97.

13 The European Parliament and Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases (O.J., June 23, 1996, L. 77) does consider that the marker's investment (in terms of financial resources, time effort or energy) in obtaining, verifying or presenting the contents of a database might be protected by a new economic right.

14 See P. Samuelson, *Technological Protection for Copyright Works*, 1996, http://www.sims.berkeley.edu/~pam/courses/cyberlaw/docs/techpro.html.

15 See Dussollier, op. cit.

16 See Appendix to this book, p.228 (para. II.A.9); and UNESCO, 'Report of the Experts Meeting on Cyberspace Law', Paris, UNESCO (CII/USP.EC7/99/01), 1999, para. II.A.9.

17 See E. Montero, 'Les responsabilités liées à la diffusion des informations illicites ou inexactes sur Internet: Internet face au droit', *Centre de Recherches Informatique et Droit*, (12), 1997, pp.111–36.

18 See J-M. Dinant, 'Les traitements invisibles sur l'Internet', *Centre de Recherches Informatique et Droit*, 1997; *idem*, 'Communication ou A-Communication? L'électronisation du commerce', *Revue Générale*, (3), 1999, pp.39–47; and J. Reidenberg, 'Les Informatica: The Formulation of Information Policy Rules through Technology', *Texas Law Review*, **3**, February, 1998, pp.553ff.

19 On all these points see S. Louveaux, Y. Poullet and A. Salaun, *User Protection in*

the Cyberspace: Some Recommendations, 1999, http://www.jura.uni-muenster.de/eclip.

20 See Reidenberg, 'Governing Networks', op. cit.

21 See Y. Poullet and R. Queck, 'Le droit face à Internet, Internet face à droit', *Cahiers du CRID, (Centre de Recherches Informatique et Droit)*, (12), 1997, pp.231–49.

22 See Dinant, 'Communication ou A-Communication?', op. cit.

23 See Poullet and Queck, 'Le droit face à Internet', op. cit.

24 See Trudel et al., *Droit du cyberspace*, op. cit.

25 See Poullet, 'Le droit de l'informatique', op. cit.

26 See B. Frydman, *Quel droit pour l'Internet, Internet sous le regard du droit*, Brussels: Editions du Jenne Barreau, 1997.

27 For example, J-J. Avenue, 'Cyberspace et droit international: pour un nouveau jus communicationis', *Revue de la Recherche Juridique – Droit prospectif*, 1996, pp.811–44.

28 See R. Dunne, 'Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm', *Jurimetrics Journal*, (35), 1994, pp.11ff; P. Trudel 'Le cyberespace: réseaux constituants et réseau de réseaux', in J. Frémont and J-P. Ducasse (eds), *Les autoroutes de l'information: enjeux et défis*, Montreal: Les chemins de recherche, 1996, pp.137–59.

29 P. Trudel, 'Les effets juridiques de l'autoréglementation', *Revue de droit de l'Université de Sherbrooke*, 19, 1988–89, pp.247–86.

30 See P. Trudel, op. cit., p.251, quoting V. Cerf, *Guidelines for Conduct on and Use of Internet*, 14 August 1994 at http://info.isoc.org:80/policy/conduct/cerf-Aug-draft/html.

31 See T.I. Hardy, 'The Proper Legal Regime for "Cyberspace"', *University of Pittsburgh Law Review*, (55), 1994, pp.993–1055.

32 See H.H. Perritt, 'Dispute Resolution in Electronic Networks Communities', *Villanova Law Review*, (38), 1993, pp.349–401; Dunne, 'Deterring Unauthorized Access', op. cit.

33 See D. Johnson and D. Post, *Law and Borders: The Rise of Law in Cyberspace*, http:/www.cli.org/X0025 LBFIN.html.

34 See A. Wilkinson, *An Agenda for Industry Self Regulation*, Address to Mundo Internet 98, Madrid, 19 February 1998 available at http://www.Ispo.eec.be/eif/nextgen/mundoint.html.

35 See Poullet and Royen, 'Rapport de l'atelier', op. cit.

36 See A. Rinaldi, *The Net: User Guidelines and Netiquette*, http://www.fau.edu/rinaldi/net/index.html.

37 See B. Wittes, 'Law in Cyberspace: Witnessing the Birth of a Legal System on the Net', *Legal Time*, (36), 1995, pp.27ff.

38 See Frydman, *Quel droit pour l'Internet*, op. cit.; J.N. Brouir and P. Martens, *Liberté, droits et réseaux dans la société de l'information*, Paris and Brussels: Brugland, LGDJ, 1996.

39 B. Frydman, *Quel droit pour l'Internet*, op. cit.

40 Trudel, 'Les effets juridiques', op. cit.

41 F. Rigaux, *Droit public et droit privé dans les relations internationales*, Paris: Pedone 1977; S. Romano, *L'ordre junidique*, Paris: Dalloz.

42 Rigaux, *Droit public*, op. cit., p.439.

43 M. Vivant, 'Cybermonde: droit et droits des réseaux', *Semaine Juridique*, (3969), 1996.

44 See J. Osman, 'Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc.: réflexions sur la dégradation des sources privées du droit', *Revue Trimestrielle de Droit Civil*, 1995, pp.509–31.

45 N. Decoopman, 'Droit et déontologie: contribution à l'étude des modes de régulation', in *Les usages sociaux du droit*, Paris: PUF, 1989.

46 See M.-H. Boulanger et al., 'La protection des données à caractère personnelle en droit communitaire', *Journal des Tribunaux de droit européen*, 1997, pp.121–7, 145–55, 173–9.

47 98/560/EC, Official Journal L270, 07/10/98, pp.0048–0055.

48 Amended proposal, presented by the Commission pursuant to Article 250 (2) of the EC-Treaty, of the proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market (1999/C 30/04), COM (1998) 586 final of 18.11.1998, OJ C 30, 5.2.1999, p.4.

49 Data Protection Working Group, Working Paper, 'Transborder Data Flows towards Third Countries', Art. 25 and 26 D.P. Direct Implementation, Document adopted 24 July 1998, XV D/5025/98 – EN W.P. 12.

50 See Vivant, 'Cybermonde' op. cit.

51 Reidenberg, 'Governing Networks' op. cit., p.911.

52 Osman, 'Avis, directives, codes de bonne conduite', op. cit., p.530.

53 Osman, op. cit., p.531.

54 C. Lamouline and Y. Poullet, op. cit., pp.112–13.

55 See E. Mackay, 'Lawyering and Litigating in Cyberspace', Address to the Eleventh Colloquium on Legal Data Processing in Europe, 4 October 1993.

56 See F. van der Mensbrugghe, 'Le service universel aux Etats-Unis', *Centre de Recherches Informatique et Droit*, (14).

57 A colloquium, 'L'information juridique: contenu, accessibilité et cirulation. Défis politiques, juridiques, économiques et techniques' (Paris, 22 and 23 October 98) organised by the French ADIJ (Association for the Development of Legal Informatics) was dedicated to the analysis of the recent national government initiatives around the diffusion of legal documents (Belgium, Canada, France, the Netherlands, USA, etc.) The texts of the different interventions are available on the ADIJ's web site: http://www.adij.assoc.fr.

58 Taken up here are certain ideas that were developed in Chapter 3 of Lamouline and Poullet, *Des autoroutes d'information*, op. cit.

59 See B. Wellman and M. Gulia (1998), 'Net Surfers don't Ride Alone: Virtual Community as Community in Networks in the Global Village', Barney Wellman (ed.), (available at http://www.acm.org/ccp/references/wellman/wellman.html).

60 S. Rodota, 'Démocratie électronique: rapport générale par la Conseil de l'Europe', *Séminaire sur la demande électronique*, Paris, Palais du Luxembourg Senate, 23–24 March 1995.

61 See P. Levy, *Cyberculture: Report to the Council of Europe*, Paris: Odile Jacob, 1997, pp.228ff.

62 See S. Rodota, 'Technopolitica: La democrazia e la nuove technologie della communicazione', *Sagitari Laterza*, Rome, 1997.

BIBLIOGRAPHY

Antoine, M. and Gobert, D. (1998), 'Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification', *Revue Générale de Droit Civil*, pp.285–310.

Brouir, J.N. and Martens, P. (1996), in *Liberté, droits et réseaux dans la société de l'information*, Paris/Bruxelles: LGDJ. Brugland.

Cerf, V. (1994), *Guidelines for Conduct on and Use of Internet*, 14 August 1994, available at http://info.isoc.org:80/policy/conduct/cerf-Aug-draft/html.

Couret, A., Igalens, J. and Penan, H. (1995), *La certification*, Paris: PUF.
Davio, E. (1997), 'Questions de certification, signature et cryptographie, Internet face au droit', *Cahiers du CRID (Centre de Recherches Informatiques et Droit)*, (12), pp.65–86.
Decoopman, N. (1989), 'Droit et déontologie : contribution à l'étude des modes de régulation', in: *Les usages sociaux du droit*, Paris: PUF, pp.87–105.
Dinant, J-M. (1997), 'Les traitements invisibles sur Internet', *Centre de Recherches Informatiques et Droit*, 7pp.
Dinant, J-M. (1998), *Using PICS as an Enhancing Privacy Technology*, http://www.droit.fundp.ac.be/crid/eclip/pics.html.
Dinant, J-M. (1999), 'Communication ou A-Communication? L'électronisation du commerce', *Revue Générale*, (3), pp.39–47.
Dunne, R. (1994), 'Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace through a Contract Law Paradigm', *Jurimetrics Journal*, (35), pp.11ff.
Dussollier, S. (1999), 'Electrifying the Fence: The Legal Protection of Technological Measures for Protecting Copyright', *European Intellectual Property Review*, pp.285–97.
Electronic Frontier Foundation (EFF) (1995), *General Information about the Electronic Frontier Foundation*, Washington DC, 20pp., http://www.eff.org/EFFdocs/about_eff.html #INTRO.
Frydman, B. (1997), *Quel droit pour l'Internet, Internet sous le regard du droit*, Colloquium of 15 November 1997, Brussels: Editions du Jeune Barreau, p.295ff.
Hardy, T.I. (1994), 'The Proper Legal Regime for "Cyberspace"', *University of Pittsburgh Law Review*, (55), pp.993–1055.
Johnston, D. and Post, D. (1996), *Laws and Borders: The Rise of Law in Cyberspace*, http://www.cli.org/X0025_LBFIN.html.
Lamouline, C. and Poullet, Y. (1997), *Des autoroutes de l'information à la démocratie électronique*, Bruylant. Report to the Council of Europe, Brussels: Nemesis.
Lavenue, J-J. (1996), 'Cyberspace et droit international : pour un nouveau jus communicationis', *Revue de la Recherche Juridique – Droit Prospectif*, pp.811–44.
Levy, P. (1997), *Cyberculture: Report to Council of Europe*, Paris: Odile Jacob, pp.228ff.
Louveaux, S., Poullet, Y. and Salaun, A. (1999), *User Protection in the Cyberspace: Some Recommendations*, http://www.jura.uni-muenster.de/eclip.
Mackay, E. (1993), 'Lawyering and Litigating in Cyberspace', Address to the Eleventh Colloquium on Legal Data Processing in Europe, 4 October.
Mensbrugghe, F. van der (1998), 'Le service universel aux Etats-Unis', *CRID* (14).
Montero, E. (1997), 'Les responsabilités liées à la diffusion d'informations illicites ou inexactes sur Internet: Internet face au droit', *CRID*, (12), pp.111–36.
Montero, E. (1998), *La responsabilité du fait des informations accessibles en ligne*, Namur: PUN.
Osman, F. (1995), 'Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc.: réflexions sur la dégradation des sources privées du droit', *Revue Trimestrielle de Droit Civil*, pp.509–31.
Perritt, H.H., jr (1992), 'The Electronic Agency and the Traditional Paradigms of Administrative Law', *Administrative Law Review*, **44**, pp.79–105.
Perritt, H.H., jr (1993), 'Dispute Resolution in Electronic Networks Communities', *Villanova Law Review*, (38), pp.349–401.
Perritt, H.H., jr (1996), 'Jurisdiction in Cyberspace : The Role of Intermediaries', *Symposium on Information, National Policies and International Infrastructure*, 28–30 January 1996, Harvard, http://www.law.vill.edu/harvard/article/harv96k.htm.
Post, D. (1995), 'Anarchy, State and the Internet : An Essay on Law-Making in Cyberspace', *Journal of Online Law*, art. 3, http://www.law.cornell.edu/jol/post.html.

Poullet, Y. (1993), 'Le droit de l'informatique existe-t-il?' in: *Droit de l'informatique : enjeux-nouvelles responsabilités*, Brussels: Conférence du Jeune Barreau, pp.1–43.
Poullet, Y. and Havelange, B. (1998), *Preparation of a Methodology for Evaluating the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data*. Annex to Annual Report 1998, XV D/5047/98, Brussels: Office for Official Publication of the European Communities.
Poullet, Y. and Queck, R. (1997), 'Le droit face à Internet, Internet face au droit', *Cahiers du CRID (Centre de Recherches Informatique et Droit)*, (12), pp.231–49.
Poullet, Y. and Royen, J. (1998), 'Rapport de l'atelier : Commerce électronique : vers la confiance', *AGORA*, (98), 16 December, 73 pp.
Reidenberg, J. (1996), 'Governing Networks and Cyberspace Rule-Making', *Emory Law Journal*, p.911. Also available at *Symposium on Information, National Policies and International Infrastructure*, 28–30 January 1996, Harvard, http://ksgwwwharvard.edu/~itbspp/reidpap2.htm.
Reidenberg, J. (1998), 'Lex Informatica: The Formulation of Information Policy Rules through Technology', *Texas Law Review*, 3, February, pp.553ff.
Rigaux, F. (1977), *Droit public et droit privé dans les relations internationales*, Paris: Pedone.
Rigaux, F. (1997), 'Le droit au singulier et au pluriel', *Revue Interdisciplinaire d'Etudes Juridiques*, (9), pp.45ff.
Rinaldi, A. (1995), 'The Net: User Guidelines and Netiquette', http://www.fau.edu/rinaldi/net/index.html.
Rodota, S. (1995), 'Démocratie électronique: rapport général par le Conseil de l'Europe', *Séminaire sur la demande électronique*, Paris: Senate, Palais du Luxembourg, 23–24 March.
Rodota, S. (1997), 'Technopolitica: La democrazia e le nuove technologie della communicazione', *Sagitari Laterza*, Rome.
Romano, S. (1975), *L'ordre juridique*, Paris: Dalloz.
Samuelson, P. (1996), *Technological Protection for Copyright Works*, http://www.sims.berkeley.edu/~pam/courses/cyberlaw/docs/techpro.html.
Trudel, P. (1988–89), 'Les effets juridiques de l'autoréglementation', *Revue de droit de l'Universite de Sherbrooke*, **19**, pp.247–86.
Trudel, P. (1996), 'Le cyberespace : réseaux constituants et réseau de réseaux', in: J. Frémont and J-P. Ducasse (eds), *Les autoroutes de l'information : enjeux et défis*. Montréal: Les chemins de la recherche, pp.137–59. (Actes du Colloque tenu dans le cadre des Huitièmes entretiens Centre Jacques Cartier, Rhône-Alpes, 5–8 December 1995.)
Trudel, P. et al. (1997), *Droit du cyberspace*, Montreal: Université de Montréal/Editions Thémis.
Vivant, M. (1996), 'Cybermonde: droit et droits des réseaux', *Semaine Juridique*, (3969).
Wellman, B. and Gulia, M. (1998), 'Net Surfers don't Ride Alone: Virtual Community as Community in Networks in the Global Village', Barney Wellman (ed.), (available at http://www.acm.org/ccp/references/wellman/wellman.html).
Wilkinson, A. (1998), *An Agenda for Industry Self Regulation*, Address to Mundo Internet 98, Madrid, 19 February 1998, available at http://www.Ispo.eec.be/eif/nextgen/mundoint.html.
Wittes, B. (1995), 'Law in Cyberspace: Witnessing the Birth of a Legal System on the Net, *Legal Time*, (36), pp.27ff.